UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ANDREW CHERNEY AND JACK CHERNEY, individually and on behalf of all others similarly situated,	Case No. 17-cv-12966
Plaintiffs,	Hon.
-v.-	**CLASS ACTION COMPLAINT**
EQUIFAX, INC.,	**JURY TRIAL DEMANDED**
Defendant.	

David H. Fink (P28235)
Darryl Bressack (P67820)
Nathan J. Fink (P75185)
FINK + ASSOCIATES LAW
Attorneys for Plaintiffs
38500 Woodward Ave., Ste. 350
Bloomfield Hills, MI 48304
Tel.: (248) 971-2500
dfink@finkandassociateslaw.com
dbressack@finkandassociateslaw.com
nfink@finkandassociateslaw.com

CLASS ACTION COMPLAINT

Plaintiffs, Andrew Cherney and Jack Cherney ("Plaintiffs"), bring this nationwide class action on behalf of themselves and all other persons similarly situated against Defendant Equifax, Inc. ("Equifax"). Plaintiffs allege the following

upon information and belief, except for those allegations that specifically pertain to Plaintiffs, which are based on Plaintiffs' personal knowledge.

INTRODUCTION

1. This national class action complaint seeks monetary and nonmonetary relief on behalf of over 140 million individuals across the country who were harmed by Equifax, Inc.'s failure to adequately protect credit reports and personal information. Unidentified hackers exploited a security vulnerability in the U.S. web site for Equifax. As a result of the breach, unauthorized persons gained access to personal information belonging to more than 140 million individuals in the United States. According to Equifax, the data exposed in the breach includes highly sensitive information, including names, birthdates, addresses, social security numbers, and driver's license numbers.

PARTIES

2. Andrew Cherney is a citizen of the State of Michigan. Plaintiff Andrew Cherney has confirmed that his sensitive personal information was impacted by the data breach.

3. Jack Cherney is a citizen of the State of Michigan. Plaintiff Jack Cherney has confirmed that his sensitive personal information was impacted by the data breach.

4. Defendant Equifax, Inc. ("Equifax") is a multi-billion dollar Georgia corporation. Headquartered in Atlanta, Georgia, Equifax is one of three primary credit bureau reporting agencies in the United States.

5. On September 7, 2017, Equifax issued a press release relating to the data breach, stating as follows:

> Equifax today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. web site application vulnerability to gain access to certain to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The Company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence of personal information of consumers in any other country has been impacted.
>
> Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated web site, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian, and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern Time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulatory inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

> CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize that we must do more. And we will."

JURISDICTION AND VENUE

6. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). Plaintiffs and numerous members of the putative class are citizens of a state different than Defendant, the amount in controversy exceeds $5,000,000.00, and there are more than 100 putative Class members.

7. This Court has personal jurisdiction over Equifax because Equifax regularly conduct business in Michigan, maintains credit reports on consumers who live in Michigan, and has sufficient minimum contacts in Michigan.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Equifax does business in this District and substantial events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

9. Equifax is one of the largest consumer credit reporting agencies in the United States. According to its web site, Equifax gathers and maintains information on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data compiled from more than 7,100

employers of consumers and businesses. In 2016, Equifax's operating revenue exceeded $3.1 billion.

10. As part of its business model, Equifax collects personally identifiable information ("PII") pertaining to millions of consumers and businesses, including but not limited to names, birthdates, social security numbers, addresses, credit card numbers, student loan information, revolving credit account histories, account payment histories, and driver's license information.

11. In addition, Equifax collects dispute applications filed by consumers who disagree with certain information pertaining to the individual credit reports that Equifax has generated for them.

12. Equifax has a legal duty to use every means available to protect stored PII from falling into the hands of identity thieves and other criminals.

13. For some period of time between May 2017 and July 2017, unidentified computer hackers gained access to Class members' PII by exploiting a security vulnerability in Equifax's web application.

14. Equifax states that on July 29, 2017, the company discovered that hackers had gained access to Class members' PII.

15. Equifax did not publicly disclose this security breach until September 7, 2017, when it issued press releases.

16. Various media outlets have reported that certain Equifax executives sold company shares between the time the company learned of the data breach and the time the information was made public.

17. Equifax's September 7, 2017, press release acknowledges that the data breach affected as many as 143 million Americans. The PII exposed in the hack includes some of the most sensitive of all personal information, including but not limited to names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers.

18. Equifax's September 7, 2017, press release also acknowledges that the hackers accessed credit card numbers pertaining to approximately 209,000 Americans, and credit report dispute documents with PII pertaining to approximately 182,000 Americans.

19. PII, including that pertaining to Plaintiffs and the proposed Class members, is valuable.

20. The Federal Trade Commission ("FTC") warns consumers to pay particular attention to how they keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft."

21. The information stolen from Equifax, including Plaintiffs' and Class members' personal and/or financial information, is extremely valuable to thieves. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

22. Personal and financial information such as that stolen in the Equifax data breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetrate more and larger thefts.

23. The ramifications of Equifax's failure to keep Plaintiffs' and Class members' personal and/or financial information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, social security number, date of birth, and other information, without permission, to commit fraud or other crimes.

24. Identity thieves can use personal information such as that pertaining to Plaintiffs and the class, which Equifax failed to keep secure, to perpetrate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or

identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

25. This is not the first time that Equifax has failed to adequately protect the personal information of its customers. For example, in March 2013, Equifax confirmed that fraudulent and unauthorized access to four consumer credit reports had occurred through the AnnualCreditReport.com web site. News outlets reported that personal details belonging to several well-known individuals – including former U.S. Secretary of State Hillary Clinton, former U.S. Vice President Joseph Biden, and celebrity musicians Jay-Z and Beyonce Knowles – were exposed during that breach.

PLAINTIFFS' FACTUAL ALLEGATIONS

26. Plaintiffs Andrew Cherney and Jack Cherney are individuals whose credit reports containing sensitive PII were maintained by Equifax. When they engaged in activities requiring hard card inquiries or that otherwise generated credit report information, Plaintiffs reasonably believed that Equifax would safeguard this sensitive personal and/or financial information in a secure manner.

27. Plaintiffs' PII was compromised in and as a result of the 2017 Equifax data breach. They were harmed by having their financial and personal information compromised and face the imminent threat of future additional harm from the increased risk of identity theft and fraud due to the financial and personal information being sold on the internet black market and misused by criminals.

CLASS ACTION ALLEGATIONS

28. Pursuant to Federal Rule 23, Plaintiffs brings the claims that Equifax violated data breach statutes (Count I) on behalf of separate state classes in and under the respective data breach statutes of all fifty states except Alabama and South Dakota, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. These classes are defined as follows:

State Data Breach Statute Classes:

> All residents of [name of State or jurisdiction] whose personal information was compromised or placed at risk or who had to pay for third-party credit monitoring services as a result of the Equifax data breach first publicly reported on September 7, 2017.

29. Pursuant to Federal Rule 23, Plaintiffs bring separate claims for violations of state data breach statutes (Count I) and negligence (Count II) on behalf of the respective state classes in and under the laws of each respective State or other jurisdiction of the United States as set forth in Counts II, III, and IV. These classes for each of the foregoing claims are defined as follows:

State Common Law Classes [Negligence]:

> All residents of [name of State or jurisdiction] whose personal information was compromised or placed at risk or who had to pay for third-party credit monitoring services as a result of the Equifax data breach first publicly reported on September 7, 2017.

30. Excluded from each of the above Classes are Equifax, including any entity in which Equifax has a controlling interest or is a parent or subsidiary, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Equifax. Also excluded are attorneys for the Classes, the judges and court personnel in this case and any members of their immediate families.

31. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same exclusive and common evidence as would be used to prove those elements in individual actions alleging the same claims.

32. All members of the purposed Classes are readily ascertainable. Equifax has access to addresses and other contact information for members of the Classes, which can be used for providing notice to many Class members.

33. **Numerosity.** Plaintiffs do not know the exact number of Class members but believes that the Class comprises more than 140 million individual consumers throughout these United States. As such, Class members are so numerous that joinder of all members is impracticable.

34. **Commonality and predominance**. Well-defined, nearly identical legal or factual questions affect all Class members. These questions predominate over questions that might affect individual Class members. These common questions include, but are not limited to, the following:

a. Whether there was an unauthorized disclosure by Equifax of Class members' personal and/or financial information;

b. Whether Equifax enabled an unauthorized disclosure of Class members' personal and/or financial information;

c. Whether Equifax misrepresented the safety and security of Class members' personal and/or financial information maintained by Defendants;

d. Whether Equifax implemented and maintained reasonable procedures and practices appropriate for maintaining the safety and security of Class members' personal and/or financial information;

e. When Equifax became aware of an unauthorized disclosure of Class members' personal and/or financial information;

f. Whether Equifax unreasonably delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

g. Whether Equifax intentionally delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

h. Whether Equifax's conduct was negligent;

i. Whether Equifax's conduct was deceptive;

j. Whether Equifax's conduct was knowing, willful, intentional, and/or malicious;

k. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

35. **Typicality**. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class members were injured through Equifax's misconduct described above and assert the same claims for relief. The same events and conduct that give rise to Plaintiffs' claims are identical to those that give rise to the claims of every other class member because Plaintiffs and each Class member have suffered harm as a direct result of the same conduct (and omissions of material facts) engaged in by Defendant and resulting in the Equifax data breach.

36. **Adequacy**. Plaintiffs will fairly and adequately protect Class members' interests. Plaintiffs have no interests antagonistic to Class members' interests, and Plaintiffs have retained counsel that has considerable experience and success in prosecuting complex class action and consumer protection cases.

37. **Superiority**. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class members. Plaintiffs and the Class members have been harmed by Equifax's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Equifax's wrongful actions and inaction.

38. A class action is an appropriate method for the fair and efficient adjudication of this controversy. There is no special interest in the members of the Class individually controlling the prosecution of separate actions. The loss of money and other harm sustained by many individual Class members will not be large enough to justify individual actions, especially in proportion to the significant costs and expenses necessary to prosecute this action. The expense and burden of individual litigation makes it impossible for many members of the Class individually to address the wrongs done to them. Class treatment will permit the adjudication of claims of Class members who could not afford individually to litigate their claims against Defendant. Class treatment will permit a large number of similarly situated persons to prosecute their common claims in a single form simultaneously, efficiently, and without duplication of effort and expense that numerous individual actions would entail. No difficulties are likely to be encountered in the management of this class action that would preclude its maintenance as a class action, and no superior alternative exists for the fair and efficient adjudication of this controversy.

39. Class certification, therefore, is appropriate under Federal Rules 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Classes, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

40. Class certification is also appropriate under Federal Rules 23(a) and (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

41. The expense and burden of litigation will substantially impair the ability of Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Defendant will retain the benefits of its wrongdoing despite serious violations of the law.

COUNT I

VIOLATIONS OF STATE DATA BREACH STATUTES
(On behalf of Plaintiffs and the State Data Breach Statute Classes.)

42. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

43. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the jurisdiction that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the

system to any resident of the jurisdiction whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

44. The Equifax data breach constitutes a breach of the security system of Equifax within the meaning of the below data breach statutes and the data breached is protected and covered by the below data breach statutes.

45. Plaintiffs and Class members' names, birthdates, social security numbers, credit dispute histories, street addresses, and driver's licenses constitute personal information under and is subject to the below data breach statutes.

46. Equifax unreasonably delayed in informing the public, including Plaintiffs and members of the State Data Breach Statute Classes about the breach of security of Plaintiffs' and Class members' confidential and non-public personal information after Equifax knew or should have known that the data breach had occurred.

47. Equifax failed to disclose to Plaintiffs and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiffs' and Class members' personal and financial information when Defendant knew or reasonably believed such information had been compromised.

48. Plaintiffs and members of the Class suffered harm directly resulting from the delay in Equifax providing timely and accurate notice as required by the

below data breach statutes. Plaintiffs, like all other Class members, suffered damages as a direct result of Equifax's delay in providing timely and accurate notice of the data breach.

49. Had Defendant provided timely and accurate notice of the data breach, Plaintiffs and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Defendant in providing notice.

50. Equifax's failure to provide timely and accurate notice of the Equifax data breach violated the following data breach statutes where Defendant does substantial business:

1. Alaska Stat. § 45.48.010 *et seq.*;
2. Arizona Rev. Stat. § 18-545 *et seq.*;
3. Ark. Code §§ 4-110-101 *et seq.*;
4. Cal. Civ. Code §§ 1798.29, 1798.83(a), *et seq.*;
5. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;
6. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;
7. Del. Code tit. 6, § 12B-101, *et seq.*;
8. Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i), *et seq.*;
9. Ga. Code Ann. § 10-1-910, 911 and 912, *et seq.*;
10. Haw. Rev. Stat. § 487N-1, *et seq.*;

11. Idaho Stat. §§ 28-51-104 to -107, *et seq.*;

12. Illinois 815 ILCS §§ 530/1 to 530/25;

13. Ind. Code §§ 4-1-11, *et seq.*, 24-4.9, *et seq.*;

14. Iowa Code §§ 715C.1, 715C.2;

15. Kan. Stat. § 50-7a01 *et seq.*;

16. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

17. La. Rev. Stat. §§ 51:3071, *et seq.*;

18. Me. Rev. Stat. tit. 10 § 1346, *et seq.*;

19. Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308;

20. Mass. Gen. Laws § 93H-1, *et seq.*;

21. Mich. Comp. Laws §§ 445.63, 445.72;

22. Minn. Stat. §§ 325E.61, 325E.64;

23. Miss. Code § 75-24-29;

24. Mo. Rev. Stat. § 407.1500, *et seq.*;

25. Mont. Code §§ 2-6-1501 to -1503, 30-14-1701, *et seq.*, 33-19-321;

26. Neb. Rev. Stat. §§ 87-801, *et seq.*;

27. Nev. Rev. Stat. §§ 603A.010, *et seq.*, 242.183;

28. N.H. Rev. Stat. §§ 359-C:19, *et seq.*;

29. N.J. Stat. § 56:8-161, *et seq.*;

30.New Mexico 2017 H.B. 15, Chap. 36;

31.N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208;

32.N.C. Gen. Stat §§ 75-61, 75-65;

33.N.D. Cent. Code §§ 51-30-01 *et seq.*;

34.Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192;

35.Okla. Stat. §§ 74-3113.1, 24-161 to -166;

36.Oregon Rev. Stat. §§ 646A.600 to .628;

37.Pa. - 73 Pa. Stat. §§ 2301, *et seq.*;

38.R.I. Gen. Laws §§ 11-49.3-1, *et seq.*,

39.S.C. Code § 39-1-90;

40.Tenn. Code §§ 47-18-2107; 8-4-119;

41.Tex. Bus. & Com. Code §§ 521.002, 521.053;

42.Utah Code §§ 13-44-101, *et seq.*;

43.Vt. Stat. tit. 9 §§ 2430, 2435;

44.Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

45.Wash. Rev. Code §§ 19.255.010, 42.56.590;

46.W.V. Code §§ 46A-2A-101, *et seq.*;

47.Wis. Stat. Ann. § 134.98(2), *et seq.*;

48.Wyo. Stat. §§ 40-12-501 *et seq.*;

49.D.C. Code §§ 28- 3851 *et seq.*;

50. Guam - 9 GCA §§ 48-10 *et seq.*;

51.Puerto Rico - 10 Laws of Puerto Rico §§ 4051 *et seq.*;

52.U.S. Virgin Islands - V.I. Code tit. 14, §§ 2208, 2209;

51. Plaintiffs and members of each of the State Data Breach Statute Classes seek all remedies available under their respective data breach statutes, including but not limited to a) damages suffered by Plaintiffs and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT II

NEGLIGENCE

(On behalf of Plaintiffs and the separate State Negligence Classes.)

52. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

53. Defendant came into possession, custody, and/or control of personal and/or financial information of Plaintiffs and Class members.

54. Defendant owed a duty to Plaintiffs and members of the State Negligence Classes to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiffs and Class members.

55. Defendant had a duty to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the

safety and security of Plaintiffs' and Class members' personal and/or financial information in their possession, custody, and/or control.

56. Defendant had a duty to exercise reasonable care in timely notifying Plaintiffs and Class members of an unauthorized disclosure of personal and/or financial information.

57. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiffs and Class members.

58. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiffs' and Class members' personal and/or financial information.

59. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in timely notifying Plaintiffs and Class members of an unauthorized disclosure of their personal and/or financial information.

60. Defendant's negligent and wrongful breach of duties owed to Plaintiffs and Class members proximately caused an unauthorized disclosure of Plaintiffs and Class members' personal and/or financial.

61. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class have suffered injury, are entitled to equitable relief in the form of an accounting of exactly how their credit and personal information was accessed without authorization by third parties, restitution, damages in an amount to be proven at trial, attorneys' fees and costs, and unless agreed upon by Equifax, an order to preserve all documents and information (and electronically stored information) pertaining to this case.

62. Wherefore, Plaintiffs prays for relief as set forth below.

PRAYER FOR RELIEF

On behalf of themselves and the Classes set forth above, Plaintiffs request the Court order relief and enter judgment against Defendant and enter an order:

A. certifying this case as a class action pursuant to Federal Rules 23(a), (b)(2), and (b)(3), and, pursuant to Federal Rule 23(g), appoint the named Plaintiffs to be Class representative and the undersigned counsel to be Class counsel;

B. requiring Defendant to make whole any losses suffered by Plaintiffs and Class members;

C. requiring Defendant to protect and indemnify Plaintiffs and Class members from any present or future harm caused by Defendant's actions;

D. enjoining Defendant from further engaging in the unlawful conduct complained of herein;

E. requiring Defendant to institute procedures and protocols to better protect PII from theft or future disclosure;

F. awarding Plaintiffs and the Classes appropriate relief, including actual and statutory damages, restitution, and disgorgement;

G. awarding pre-judgment and post-judgment interest;

H. requiring Defendant to pay for notifying the Class of the pendency of this action;

I. requiring Defendant to pay Plaintiffs and Class members reasonable attorneys' fees, expenses, and the costs of this action; and

J. providing all other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury on all issues so triable.

DATED this 8th day of September, 2017.

Respectfully submitted,

FINK + ASSOCIATES LAW

/s/ David H. Fink
David H. Fink (P28235)
Darryl Bressack (P67820)
Nathan J. Fink (P75185)
38500 Woodward Ave.; Suite 350
Bloomfield Hills, Michigan 48304
(248) 971-2500
(248) 971-2600 (fax)
dfink@finkandassociateslaw.com
dbressack@finkandassociateslaw.com
nfink@finkandassociateslaw.com

Attorneys for Plaintiffs